日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　４月１１日

出願番号
Application Number: 特願２００２－１０９７１４

[ST.10/C]: [ＪＰ２００２－１０９７１４]

出願人
Applicant(s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年　４月１１日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０２５４６４

【書類名】　特許願
【整理番号】　JP9020047
【提出日】　平成14年 4月11日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/00
【発明者】
【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
【氏名】　尾家　正樹
【特許出願人】
【識別番号】　390009531
【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション
【代理人】
【識別番号】　100086243
【弁理士】
【氏名又は名称】　坂口　博
【代理人】
【識別番号】　100091568
【弁理士】
【氏名又は名称】　市位　嘉宏
【代理人】
【識別番号】　100106699
【弁理士】
【氏名又は名称】　渡部　弘道
【復代理人】
【識別番号】　100104880
【弁理士】
【氏名又は名称】　古部　次郎

【選任した復代理人】

【識別番号】　100100077

【弁理士】

【氏名又は名称】　大場　充

【手数料の表示】

【予納台帳番号】　081504

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンピュータ装置、コンピュータ装置のセキュリティ設定方法、プログラム

【特許請求の範囲】

【請求項１】　他のデバイスとの間で通信可能なコンピュータ装置であって

前記他のデバイスとの通信を介し当該他のデバイスの識別情報を取得する識別情報取得手段と、

取得した前記識別情報に基づいて、前記コンピュータ装置の使用環境を判定する使用環境判定手段と、

判定された前記コンピュータ装置の使用環境に基づき、当該コンピュータ装置の設定を変更する設定変更手段と、

を備えることを特徴とするコンピュータ装置。

【請求項２】　前記使用環境判定手段は、前記識別情報に基づき、前記コンピュータ装置の周囲に存在する前記他のデバイスを特定することによって当該コンピュータ装置の使用環境を判定することを特徴とする請求項１記載のコンピュータ装置。

【請求項３】　前記コンピュータ装置は、ブルートゥースによる通信を行う通信手段をさらに備え、

前記識別情報取得手段は、ブルートゥースによる通信が可能な前記他のデバイスからブルートゥース・デバイス・アドレスを前記識別情報として取得することを特徴とする請求項２記載のコンピュータ装置。

【請求項４】　前記設定変更手段は、前記コンピュータ装置の使用環境に基づき、当該コンピュータ装置のセキュリティ設定を変更することを特徴とする請求項１記載のコンピュータ装置。

【請求項５】　前記設定変更手段は、前記使用環境判定手段にて特定の使用環境にあると判定されたときには当該特定の使用環境に応じたセキュリティ設定とし、

前記特定の使用環境以外であると判定されたときには、前記特定の使用環境の

ときよりも高いセキュリティ性を有したセキュリティ設定とすることを特徴とする請求項４記載のコンピュータ装置。

【請求項６】　前記設定変更手段は、前記コンピュータ装置の使用環境に基づき、当該コンピュータ装置における消費電力を制御するための設定を変更することを特徴とする請求項１記載のコンピュータ装置。

【請求項７】　可搬性を有するコンピュータ装置が当該コンピュータ装置の使用環境に関する情報を取得するステップと、

取得した前記情報に基づいて前記コンピュータ装置が当該コンピュータ装置のセキュリティ設定を変更するステップと、

を有することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項８】　前記使用環境に関する情報を取得するステップでは、前記コンピュータ装置の周囲のデバイスから発せられる当該デバイスの識別情報を取得することを特徴とする請求項７記載のコンピュータ装置のセキュリティ設定方法。

【請求項９】　前記セキュリティ設定を変更するステップでは、前記デバイスの識別情報が予め登録されたものであるか否かに応じ、セキュリティ設定のレベルを変更することを特徴とする請求項８記載のコンピュータ装置のセキュリティ設定方法。

【請求項１０】　前記デバイスの識別情報が予め登録されたものではないとき、セキュリティ設定を高いレベルに変更することを特徴とする請求項９記載のコンピュータ装置のセキュリティ設定方法。

【請求項１１】　可搬性を有するコンピュータ装置が当該コンピュータ装置のセキュリティ設定を行う方法であって、

前記コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得するステップと、

前記デバイス情報が取得できる環境におけるセキュリティ設定の指定を受け付けるステップと、

指定された前記セキュリティ設定を前記デバイス情報に関連付けて格納するステップと、

を有することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項１２】　前記セキュリティ設定および前記デバイス情報の格納後、

前記コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得するステップと、

取得した前記デバイス情報に関連付けられた前記セキュリティ設定を呼び出すステップと、

前記コンピュータ装置を、呼び出した前記セキュリティ設定に変更するステップと、

をさらに前記コンピュータ装置が実行することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項１３】　コンピュータ装置に所定の処理を実行させるプログラムであって、

前記コンピュータ装置の周囲に存在する他のデバイスとのブルートゥースによる通信を介し、当該デバイスのアドレス情報を取得する処理と、

取得した前記アドレス情報に基づいて、前記コンピュータ装置の設定を変更する処理と、

を有することを特徴とするプログラム。

【請求項１４】　前記コンピュータ装置の設定を変更する処理では、当該コンピュータ装置のセキュリティ設定を変更することを特徴とする請求項１３記載のプログラム。

【請求項１５】　前記コンピュータ装置の設定を変更する処理では、前記アドレス情報が予め登録されたものであるか否かに応じ、前記セキュリティ設定のレベルを変更することを特徴とする請求項１４記載のプログラム。

【請求項１６】　前記コンピュータ装置の設定を変更する処理では、前記デバイスのアドレス情報が予め登録されたものではないとき、前記セキュリティ設定を高いレベルに変更することを特徴とする請求項１５記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、可搬性のあるコンピュータ装置に関し、例えばセキュリティ設定等を行うに際して用いて好適な技術に関する。

【０００２】

【従来の技術】

近年、ノートブック型のＰＣ、ＰＤＡ(Personal Digital Assistants)等、可搬性のあるいわゆるモバイル機器が広く用いられている。

ノートブック型のＰＣ(以下、単にＰＣと称する)を例に挙げると、ユーザは、例えばオフィスで無線ＬＡＮを用いてネットワークに接続していたＰＣを、自宅に持ち帰ってモデムを用いてアナログ電話回線を介してネットワークに接続し、さらに出先では携帯電話を介してネットワークに接続したりしている。

また、最近では、駅や繁華街等の特定のエリアに無線ＬＡＮ環境が提供され、このようなエリア内では、提供された無線ＬＡＮを用いてネットワークに接続することもできるようになっている。

さらに、ブルートゥースといった短距離無線通信技術も広まりつつあり、オフィス、自宅、出先等において、モデムやＬＡＮアクセスポイント、あるいは他のデバイスとの間でブルートゥースによってデータ通信を行うこともできるようになっている。

【０００３】

【発明が解決しようとする課題】

しかしながら、上記のように、１台のＰＣにおいて、オフィス、自宅(以下、これをホームと適宜称する)、出先(以下、これをモバイルと適宜称する)と使用環境が複数種にわたる場合、それぞれの場所に移動するたびに、少なくともネットワークに接続するための各種設定を行わなければならない。

この設定には、数項目から数十項目の設定を変更しなければならないため、言うまでもなく非常に面倒であり、設定の変更内容を誤った場合には、ネットワーク接続自体ができなくなってしまうという問題がある。

【０００４】

このような問題を解決するため、タスクバー等に表示されるユーティリティ上において使用環境を選択するだけで、設定がワンタッチで切り替えられるような

ものも一部で提供されている。これにより、予めそれぞれの使用環境に応じた設定をしておけば良いので、毎回面倒な設定を行う必要がなくなる。

しかし、例えば、実際にはオフィスなのにホームの設定を選択する等、ユーザが設定の変更先を誤った場合には、ネットワーク接続ができないという問題が生じる。さらに、ネットワーク接続ができたとしても、実際には出先で、セキュリティ性の高いモバイルの設定とすべき使用環境にあるのに、セキュリティ性の低いホームの設定となっている場合等、誤った設定でＰＣを使用し続けると、潜在的なセキュリティホールとなる可能性もあり、これは重要な問題である。

このようなセキュリティホールがあると、特に、無線ＬＡＮやブルートゥースを用いてネットワーク接続するような環境では、他人のデバイスからの不正アクセスを有効に防ぐことができなくなってしまうこともあるからである。

【０００５】

本発明は、このような技術的課題に基づいてなされたもので、使用環境に応じて確実に設定変更を行うことのできる技術を提供することを主たる目的とする。

また、他の目的は、よりセキュリティ性の高いネットワーク接続環境を常に確保することにある。

【０００６】

【課題を解決するための手段】

かかる目的のもと、本発明のコンピュータ装置は、他のデバイスとの通信を介して識別情報取得手段にて取得した他のデバイスの識別情報に基づき、使用環境判定手段にてコンピュータ装置の使用環境を判定する。そして、判定された使用環境に基づき、設定変更手段にて、例えばセキュリティ設定等、コンピュータ装置の設定を変更する。

このとき、使用環境判定手段では、識別情報に基づき、コンピュータ装置の周囲に存在する他のデバイスを特定することによってコンピュータ装置の使用環境を判定することができる。

また、コンピュータ装置がブルートゥースによる通信を行う通信手段を備える場合、識別情報取得手段では、ブルートゥースによる通信が可能なデバイスに対して個別に割り当てられるブルートゥース・デバイス・アドレスを、他のデバイ

スから識別情報として取得することができる。

ここで、設定変更手段では、コンピュータ装置が、例えばホームやオフィス等、特定の使用環境にあると判定されたときには、その特定の使用環境に応じたセキュリティ設定とし、出先等、特定の使用環境以外であると判定されたときには、特定の使用環境のときよりも高いセキュリティ性を有したセキュリティ設定とするのが好ましい。

また、設定変更手段では、コンピュータ装置の使用環境に基づき、コンピュータ装置における消費電力を制御するための設定を変更することもできる。

【０００７】

本発明のコンピュータ装置のセキュリティ設定方法は、コンピュータ装置の使用環境に関する情報を取得し、これに基づいてコンピュータ装置のセキュリティ設定を変更することを特徴とする。

使用環境に関する情報を取得するに際しては、コンピュータ装置の周囲のデバイスから発せられるデバイスの識別情報を取得することができる。また、これ以外に、コンピュータ装置がＧＰＳ(Global Positioning System:全地球測位システム)等を利用可能であれば、ＧＰＳによって測位される位置情報を、コンピュータ装置の使用環境に関する情報として取得することもできる。

また、セキュリティ設定を変更するに際しては、デバイスの識別情報が予め登録されたものであるか否かに応じ、セキュリティ設定のレベルを変更することができる。デバイスの識別情報が予め登録されたものではないとき、セキュリティ設定を高いレベルに変更するのである。

【０００８】

また、本発明は、コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得し、そのデバイス情報が取得できる環境におけるセキュリティ設定を指定するための外部からの入力を受け付けると、指定されたセキュリティ設定をデバイス情報に関連付けて格納することを特徴とするコンピュータ装置のセキュリティ設定方法として捉えることができる。

このような方法では、セキュリティ設定およびデバイス情報の格納後に、コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得し、

取得したデバイス情報に関連付けられたセキュリティ設定を呼び出し、呼び出したセキュリティ設定に変更することができる。

【０００９】

本発明は、コンピュータ装置に所定の処理を実行させるプログラムとして捉えることもできる。この場合、このプログラムは、コンピュータ装置の周囲に存在する他のデバイスとのブルートゥースによる通信を介し、他のデバイスのアドレス情報を取得する処理と、取得したアドレス情報に基づいてコンピュータ装置のセキュリティ設定等を変更する処理と、を有する。

【００１０】

ここで、本発明におけるコンピュータ装置は、ＰＣに限らず、ＰＤＡや、携帯電話端末、他の各種デバイスであっても良いことは言うまでも無い。

【００１１】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいてこの発明を詳細に説明する。

図１は、本実施の形態におけるノートブック型のＰＣ(コンピュータ装置)１０のデバイス構成を説明するための図である。

この図１に示すように、ＰＣ１０は、所定の制御プログラムに基づいた処理を実行するＣＰＵ１１、処理用データを格納するＲＡＭ(Random Access Memory)等のメモリ１２、ディスプレイ部(ＬＣＤ)１３に表示する画像を制御するグラフィックチップ１４が、チップセット１５に接続されている。

【００１２】

このチップセット１５は、ブリッジ回路１６に接続されている。

このブリッジ回路１６には、ＩＤＥチャンネル１７を介してＨＤＤ１８が接続される。

また、ブリッジ回路１６には、キーボード１９や図示しないマウス等のポインティングデバイスからの信号の入力に基づいたイベントを出力するコントローラ２０、ＢＩＯＳ(Basic Input/Output System)を格納したＥＥＰＲＯＭ(Electrically Erasable and Programmable ROM)２１が接続されており、キーボード１９やポインティングデバイスからの入力に応じ、ＢＩＯＳが、ＰＣ１０の各部を制

御する構成となっている。

加えて、このブリッジ回路１６は、各種の設定情報を記憶するＣＭＯＳ(Complementary Metal Oxide Semiconductor)２２を内蔵し、ＣＭＯＳ２２はバッテリー２３によって、常時電源が供給されるようになっている。

【００１３】

また、ブリッジ回路１６には、ＵＳＢ(Universal Serial Bus)２４を介し、ブルートゥース通信コントローラ(識別情報取得手段、通信手段)３０が接続され、ＰＣＩ(Peripheral Component Interconnect)バス２５を介し、有線ＬＡＮ通信コントローラ３１、無線ＬＡＮ通信コントローラ３２、モデム３３が接続されている。

ブルートゥース通信コントローラ３０は、アンテナ３４を介し、他のブルートゥース対応のデバイスとの間で短距離無線通信によるデータ通信を制御する。このブルートゥース通信コントローラ３０では、アンテナ３４で送受信する電波が届く範囲内(一般に１０～１００ｍ以内)に存在する他のブルートゥース対応のデバイスとの通信を制御する。また、ブルートゥース対応のデバイスは、電源が入っている限り、ブルートゥース・デバイス・アドレス（以下、ＢＤアドレス)を含む電波を発している。ブルートゥース通信コントローラ３０は、アンテナ３４で受信した電波にＢＤアドレスが含まれる場合、これを検出する機能を備えている。

【００１４】

また、有線ＬＡＮ通信コントローラ３１は、ジャック３５に接続したＬＡＮケーブル(図示無し)を介して有線で外部のネットワーク５０にアクセスし、ネットワーク５０を介した他のコンピュータ装置とのデータ通信を制御する。

無線ＬＡＮ通信コントローラ３２は、アンテナ３６を介して無線で外部のネットワーク５０にアクセスし、ネットワーク５０を介した他のコンピュータ装置とのデータ通信を制御する。

また、モデム３３は、ジャック３７に接続したケーブル(図示無し)からアナログ回線網を介してネットワーク５０にアクセスし、ネットワーク５０を介した他のコンピュータ装置とのデータ通信を制御する。

これにより、ＰＣ１０は、例えば、ブルートゥース、無線ＬＡＮ、有線ＬＡＮ、アナログ電話回線を介したネットワーク接続が可能な構成となっている。

【００１５】

ここで、有線ＬＡＮ通信コントローラ３１と無線ＬＡＮ通信コントローラ３２は、実際には一つのイーサネットチップによって実現されるものであっても良い。また、ブルートゥース通信コントローラ３０、有線ＬＡＮ通信コントローラ３１、無線ＬＡＮ通信コントローラ３２、モデム３３の全てが必須ではなく、少なくともブルートゥース通信コントローラ３０を備えていればネットワーク通信機能を備えることができる。さらに、有線ＬＡＮ通信コントローラ３１、無線ＬＡＮ通信コントローラ３２、モデム３３のいずれも装備しない場合は、ブルートゥース通信コントローラ３０において短距離無線通信によってＬＡＮアクセスポイントにアクセスし、このＬＡＮアクセスポイントからネットワーク５０にアクセスさせる構成とすることが可能である。

【００１６】

このような構成を有するＰＣ１０は、ブルートゥース通信コントローラ３０の有する、電波の届く範囲内に存在する他のデバイスを認識する機能を用い、周辺に位置するデバイスの種類等からＰＣ１０の使用環境を判定し、使用環境に応じたセキュリティ設定等を自動的に行う。

図２は、上記のようなデバイス構成を有するＰＣ１０を、機能的な構成で捉えた図である。この図２に示すように、ＰＣ１０は、予めインストールされたプログラムに基づいた処理をＣＰＵ(図示無し)が実行することによって実現される機能として、環境判定部(使用環境判定手段)４０、通信設定制御部４１、セキュリティ設定制御部(設定変更手段)４２、省電力設定制御部(設定変更手段)４３を備える。

環境判定部４０は、ブルートゥース通信コントローラ３０においてブルートゥースによる通信が可能なデバイスに関する情報を収集することによって、ＰＣ１０の使用環境を判定する。

通信設定制御部４１は、環境判定部４０で判定した使用環境に合わせたネットワーク通信設定を行う。

セキュリティ設定制御部４２は、環境判定部４０で判定した使用環境に合わせたセキュリティ設定を行う。このときには、予め複数段階のセキュリティ設定に関する情報が、ＨＤＤ１８に格納されたデータによって実現されるセキュリティ設定情報格納部４４に格納されており、セキュリティ設定制御部４２では、この情報を参照することによって、使用環境に応じたセキュリティ設定を行う。

省電力設定制御部４３では、ＰＣ１０の使用環境に応じ、ＣＰＵ１１の動作速度やモニタ１３の表示を制御したり、サスペンドモードやハイバネーションモードへの移行等を制御する。

【００１７】

ここで、ＰＣ１０の使用環境の例を挙げる。

図３は、ユーザが自宅等でＰＣ１０を使用する場合の、後に本実施の形態で「ホーム」と称するセキュリティレベルを設定する使用環境である。

ユーザが自宅でＰＣ１０を使用する場合には、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、ブルートゥース対応のプリンタ１００、モデム１０１が存在するものとする。

また、図４は、ユーザが勤務先のオフィス等でＰＣ１０を使用する場合の、後に本実施の形態で「オフィス」と称するセキュリティレベルを設定する使用環境である。

ユーザがオフィスでＰＣ１０を使用する場合には、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、ブルートゥース対応のプリンタ２００、プロジェクタ２０１、ネットワーク５０にアクセスするためのＬＡＮアクセスポイント２０２が存在するものとする。

図５は、ユーザが出先にＰＣ１０を持ち出して使用する場合の、本実施の形態で後に「モバイル」と称するセキュリティレベルを設定する使用環境である。

ここで、ユーザが出先でＰＣ１０を使用する場合、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、自らが使用する他のブルートゥース対応のデバイスは所持していないものとする。すると、特に電車内や繁華街、コーヒーショップ等で、ＰＣ１０のブルートゥース用の電波が届く範囲内に、他人が所持するブルートゥース対応の、携帯電話端末３００、ＰＣ３０１(このＰＣ３０１

は上記ＰＣ１０と同じ構成である必要はない)、ＰＤＡ３０２等が存在することがある。

【００１８】

次に、上記のような、「ホーム」、「オフィス」、「モバイル」といった複数のセキュリティレベルの例を挙げる。

ここで、ブルートゥースによる通信を行う際には、セキュリティ設定として、「認証(Authentication)」、「許可(Authorization)」、「暗号化(Encryption)」の３項目がある。

「認証」とは、パス・キーと称される手入力によるキーワードの入力、あるいはリンク・キーと称される、パス・キーに基づいて自動的に生成されるキーワードにより、ブルートゥースによる通信を行うデバイス間で、相互認証を行うものである。

「許可」とは、ファイル転送や名刺交換といったサービスを行う毎にアクセスの可否をコントロールするものである。

「暗号化」とは、デバイス間でデータを転送する際に、リンク・キーから生成される暗号鍵を用い、データを暗号化するものである。

【００１９】

図６は、セキュリティレベルの設定の例を示すもので、「ホーム」＜「オフィス」＜「モバイル」の順でセキュリティ性が高くなり、ＰＣ１０から外部資源へのアクセス・外部資源からＰＣ１０へのアクセスの困難性が高くなる、つまりＰＣ１０におけるアクセス制限が厳しくなる設定となっている。

セキュリティレベルが「ホーム」の場合、他のデバイスからＰＣ１０に対する接続を行うときには、デバイスの「認証」を必須とし、「許可」については必要に応じて行い、データの「暗号化」は必須とする。また、ＰＣ１０から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」は、他のデバイス側から要求があったときに行うものとする。

セキュリティレベルが「オフィス」の場合、他のデバイスからＰＣ１０に対する接続を行うときには、業務上等で機密度の高いデータをやり取りすることが想定できるため、ここでは、デバイスの「認証」および「許可」、データの「暗号

化」を必須とする。また、ＰＣ１０から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」は、他のデバイス側から要求があったときに行うものとする。

セキュリティレベルが「モバイル」の場合、出先等では、最も高いセキュリティを確保する必要があるため、他人のデバイスからのアクセスについては、全て「拒否」する。また、ＰＣ１０から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」を必須とする。

図６に示したようなセキュリティレベルの設定は、ユーザが予め各項目の設定内容を選択することによって設定しても良いし、また予め上記のような複数段階のセキュリティレベルをデフォルトで用意しておいてもよい。

【００２０】

さて、ユーザは、自らがＰＣ１０を使用する使用環境に応じ、上記のようなセキュリティレベルの中から任意の段階を選択し、設定しておく必要がある。

これには、使用環境に応じたセキュリティ設定を行うためのアプリケーションを起動させる。

すると、図７に示すように、このアプリケーションでは、ＰＣ１０のブルートゥース通信コントローラ３０において、ブルートゥース用の電波が届く範囲内に存在するデバイスを検索する(ステップＳ１０１)。このとき、ブルートゥース用の電波が届く範囲内にブルートゥース対応のデバイスが存在していれば、そのデバイス自身の識別情報、デバイス情報、アドレス情報となるＢＤアドレスを検出(捕捉)することができる。

【００２１】

ＰＣ１０では、他のデバイスから発せられるＢＤアドレスを捕捉することによって、周囲に存在するデバイスを確定する（ステップＳ１０２）。

続いて、必要に応じ、ＰＣ１０では、モニタ１３上に、ＢＤアドレスを捕捉したデバイスに関する情報を表示し、ユーザに確認を促すこともできる。このようにすれば、その時点で捕捉されたデバイスのうち、常時電源が入っているような特定のデバイスのみをユーザが選択することもできる。

ＰＣ１０は、さらに、ユーザに対し、その場所におけるＰＣ１０のセキュリテ

ィレベルの設定を促す表示をモニタ１３上に行う(ステップＳ１０３)。

【００２２】

ユーザは、その場所(使用環境)におけるＰＣ１０のセキュリティレベルを、図６に示したような複数段階の設定の中から選択し、これを入力する。

ＰＣ１０では、入力されたセキュリティレベルの選択を受け付け、これを、検出されたデバイスのＢＤアドレスと関連付けてＨＤＤ１８等に格納することにより、セキュリティレベルの設定を登録する(ステップＳ１０４)。

例えば、図３に示したように、プリンタ１００、モデム１０１のＢＤアドレスが検出された使用環境に対し、ユーザが選択した「ホーム」というセキュリティレベルの設定を登録するのである。また、図４に示したように、プリンタ２００、プロジェクタ２０１、ＬＡＮアクセスポイント２０２が検出される使用環境では、ユーザが選択した「オフィス」というセキュリティレベルの設定を関連付けて登録する。

ところで、図７の一連の処理によって実行されるセキュリティ設定処理は、「ホーム」や「オフィス」等、ユーザがたびたび訪れる特定の場所においてのみ行えばよい。

そして、それ以外の使用環境では、「モバイル」のセキュリティレベルとするよう、ユーザが設定を行っても良いし、デフォルトでそのような設定としておいてもよい。

【００２３】

また、上記の処理において、それぞれの使用環境に応じ、ネットワーク５０を介した通信を行うための設定や、プリンタ１００や２００に応じた設定を記憶しておくこともできる。例えば、図３の例ではモデム１０１を用いるための各種設定情報、図４の例では、ＬＡＮアクセスポイント２０２を用いるための各種設定情報等である。

さらに、上記の処理において、それぞれの使用環境に応じた、省電力機能の設定を行うこともできる。例えば、セキュリティレベルとして「モバイル」が設定されるような使用環境では、消費電力をセーブするため、ＣＰＵ１１の処理速度やＨＤＤ１８の回転速度を落としたり、ＰＣ１０を持ち歩く際には使用しないＡ

Ｃアダプタの制御にのみ必要な部品への電源供給を遮断したりする等、省電力効果が最も高い設定とすることができる。

【００２４】

上記のように、使用環境に応じたセキュリティ設定を行った後は、ＰＣ１０が、以下のような処理を自動的に実行することにより、使用環境に応じたセキュリティ設定の切り替えを行う。

図８に示すように、ＰＣ１０では、システムの起動時、あるいはユーザの所定の操作によって要求がなされた時、あるいは予め設定されたタイマーによる割込み要求があった時に、ＰＣ１０のブルートゥース通信コントローラ３０において、ブルートゥース用の電波が届く範囲内に存在するデバイスを検索する(ステップＳ２０１)。すると、ブルートゥース用の電波が届く範囲内に存在するデバイスのＢＤアドレスを捕捉することができる。

【００２５】

続いて、ＰＣ１０の環境判定部４０にて、捕捉されたＢＤアドレスに基づき、その時点でのＰＣ１０の使用環境を判定する。

これにはまず、「ホーム」のセキュリティレベルに関連付けられているＢＤアドレスが、検出されたＢＤアドレスに含まれているか否かを判断する。つまり、セキュリティレベルを「ホーム」と設定すべき使用環境にあるデバイスが存在するか否かを判断するのである(ステップＳ２０２)。

その結果、「ホーム」のセキュリティレベルに関連付けられているＢＤアドレスが、検出されたＢＤアドレスに含まれていれば、環境判定部４０では、ＰＣ１０がセキュリティレベルを「ホーム」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部４２では、ＰＣ１０のブルートゥース通信コントローラ３０において実行するブルートゥース通信に際するセキュリティレベルの設定を、「ホーム」に変更する(ステップＳ２０３)。また、通信設定制御部４１では、ネットワーク５０を介した通信を行うためのＰＣ１０側の通信設定等を、ＢＤアドレスを検出したデバイス(図３の例ではモデム１０１)に応じたものに変更することもできる。さらに、ＰＣ１０側のプリンタ設定を、ＢＤアドレスを検出したデバイス(図３の例ではプリンタ１００)に応じたものに自動的に変更するこ

ともできる。

【００２６】

検出されたＢＤアドレスに、「ホーム」のセキュリティレベルの設定に関連付けられているＢＤアドレスが含まれていない場合、続いて、「オフィス」のセキュリティレベルに関連付けられているＢＤアドレスが、検出されたＢＤアドレスに含まれているか否かを判断する。つまり、セキュリティレベルを「オフィス」と設定すべき使用環境にあるデバイスが存在するか否かを判断するのである(ステップＳ２０４)。

その結果、「オフィス」のセキュリティレベルに関連付けられているＢＤアドレスが、検出されたＢＤアドレスに含まれていれば、環境判定部４０では、ＰＣ１０がセキュリティレベルを「オフィス」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部４２では、ＰＣ１０のブルートゥース通信コントローラ３０において実行するブルートゥース通信に際するセキュリティレベルの設定を、「オフィス」に変更する(ステップＳ２０５)。また、通信設定制御部４１では、ネットワーク５０を介した通信を行うためのＰＣ１０側の通信設定等を、ＢＤアドレスを検出したデバイス(図４の例ではＬＡＮアクセスポイント２０２)に応じたものに変更することもできる。さらに、ＰＣ１０側のプリンタ設定やプロジェクタ設定を、ＢＤアドレスを検出したデバイス(図４の例ではプリンタ２００やプロジェクタ２０１)に応じたものに自動的に変更することもできる。

【００２７】

さらに、検出されたＢＤアドレスに、「オフィス」のセキュリティレベルの設定に関連付けられているＢＤアドレスが含まれていない場合は、環境判定部４０では、ＰＣ１０が、セキュリティレベルを「モバイル」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部４２では、ＰＣ１０のブルートゥース通信コントローラ３０において実行するブルートゥース通信に際するセキュリティレベルの設定を、「モバイル」に変更する(ステップＳ２０６)。また、省電力設定制御部４３では、省電力効果の最も高い設定への変更を行うこともできる。

【００２８】

上述したような構成によれば、ＰＣ１０では、ブルートゥースを用い、周辺に存在するデバイスを検索することによって、ＰＣ１０の使用環境を判定し、その使用環境に応じてセキュリティレベルの設定を自動的に変更することができる。これにより、使用環境に応じたセキュリティレベルの変更を確実に行うことが可能となるので、常に最適なセキュリティ環境を確保することが可能となる。しかも、ユーザは、ＰＣ１０の使用環境が変わる毎にセキュリティ設定を変更する必要が無くなるので、ＰＣ１０の使い勝手が向上する。

さらに、使用環境を判定する処理においては、使用環境を判定する処理において、セキュリティレベルを「ホーム」や「オフィス」とすべき使用環境にＰＣがあるときであっても、無線の状態等によってその使用環境に存在すべきデバイスが検出されないときには、セキュリティ性の高い「モバイル」のセキュリティレベルに設定するようにした。これにより、フェイルセーフ機能を有していると言える。

この他、判定された使用環境に応じ、ネットワーク通信を行うための設定や、省電力設定、プリンタ設定やプロジェクタ設定等についても、同様に自動的に変更することが可能であるので、この点においても、ＰＣ１０の使い勝手を大幅に向上させることができる。

さらに、上記のような設定を行うに際し、ブルートゥースを用いるようにした。ブルートゥースの場合、周囲のデバイスの電源が入っていさえいれば、実際にＰＣ１０と周囲との間でデータ通信を行わなくてもよいので、特にセキュリティ設定を「モバイル」とするような使用環境においても、他のデバイスにＰＣ１０自身の情報を通知する必要も無く、高いセキュリティ性を保ったまま、上記効果を奏することができる。

【００２９】

なお、上記実施の形態では、図６にセキュリティレベルの例を挙げたが、あくまでもこれは一例に過ぎず、より少ない２段階、あるいは、より多い４段階以上のセキュリティレベルの設定とすることも可能であるし、「ホーム」、「オフィス」、「モバイル」といった各セキュリティレベルの内容も適宜変更することが

可能である。

また、例えば、勤務先におけるユーザの自席と、ユーザが使用する会議室等、複数の使用環境において、同じ「オフィス」のセキュリティ設定とすることも可能である。このような場合、通信設定や省電力設定については、個々の使用環境に応じた設定内容を記憶しさえすれば、使用環境に応じて設定を自動的に変更することは可能である。

【００３０】

ところで、上記実施の形態においては、使用環境を特定するために、ブルートゥースを用い、各デバイスに固有に割り当てられるＢＤアドレスを用いる構成としたが、これに限るものではない。

他に、ＰＣ１０がデータ通信を行う際に他のデバイス等とやり取りする、ＩＰアドレスや、無線や携帯電話通信網を用いる際の基地局アドレス、ＭＡＣアドレス等を用いることも可能である。ＩＰアドレスやＭＡＣアドレスの場合には、上記と同様に周辺のデバイスを特定することによって使用環境を判定することになる。また、無線や携帯電話通信網を用いる際の基地局アドレスを捕捉する場合には、実質的には基地局を特定することによってＰＣ１０が使用されている場所を特定し、これによって使用環境に応じたセキュリティ設定等を行うことになる。

ところで、ＩＰアドレスを用いる場合、ＩＰアドレスを動的に割り振る場合であっても、オフィスのフロア等、特定のエリアまでは絞り込むことができるので、これによってＰＣ１０の使用環境を判定すればよい。また、ＩＰアドレスの場合、使用環境を特定するという主旨からしても、汎用的に用いられるアドレス以外の、固有のＩＰアドレスを設定しておくのが好ましい。

また、基地局アドレスの場合のように、ＰＣ１０の使用場所を特定するという観点からすれば、ＰＣ１０にＧＰＳ(Global Positioning System)を用い、ＰＣ１０の位置を測位することによってＰＣ１０の使用環境を判定することも考えられる。

【００３１】

また、上記実施の形態で示したような、使用環境に応じたセキュリティ設定等を自動的に変更するためのプログラムは、以下のような記憶媒体の形態とするこ

ともできる。

すなわち、記憶媒体としては、コンピュータ装置に実行させる上記したようなプログラムを、ＣＤ－ＲＯＭ、ＤＶＤ、メモリ、ハードディスク等の記憶媒体に、コンピュータ装置が読み取り可能に記憶させれば良い。

これ以外にも、本発明の主旨を逸脱しない限り、上記実施の形態で挙げた構成を取捨選択したり、他の構成に適宜変更することが可能である。

【００３２】

【発明の効果】

以上説明したように、本発明によれば、使用環境に応じて確実に設定変更を行うことができ、セキュリティ性の高いネットワーク接続環境を常に確保することが可能となる。

【図面の簡単な説明】

【図１】　本実施の形態におけるコンピュータ装置の構成を示す図である。

【図２】　コンピュータ装置の、ブルートゥースを用いた設定制御に関わる構成を抽出した図である。

【図３】　セキュリティ設定を「ホーム」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図４】　セキュリティ設定を「オフィス」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図５】　セキュリティ設定を「モバイル」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図６】　複数段階のセキュリティ設定の一例を示す図である。

【図７】　セキュリティ設定を初期設定するときの処理の流れを示す図である。

【図８】　ＰＣの使用環境に応じてセキュリティ設定を変更するときの処理の流れを示す図である。

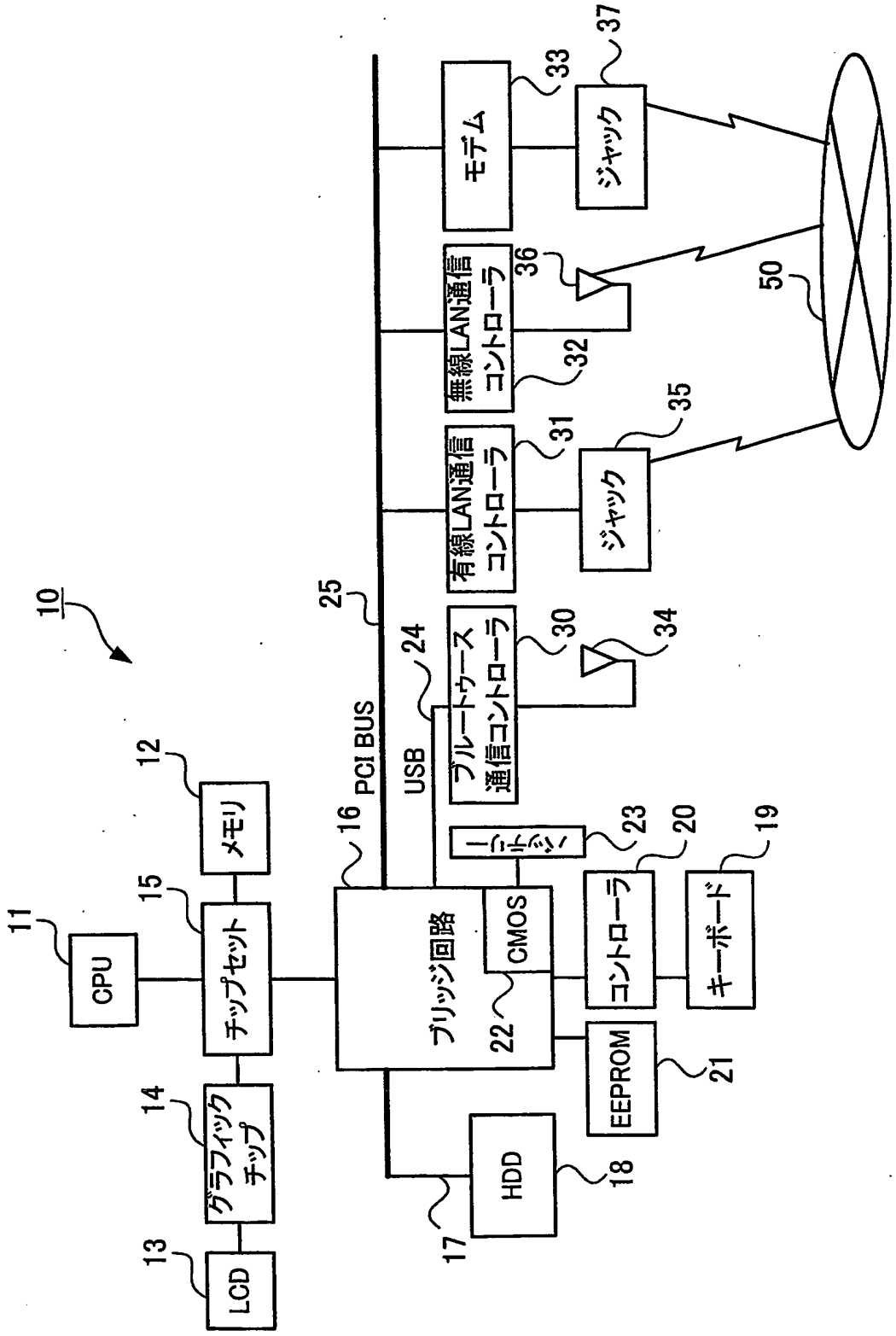
【符号の説明】

１０…ＰＣ(コンピュータ装置)、３０…ブルートゥース通信コントローラ(識別情報取得手段、通信手段)、４０…環境判定部(使用環境判定手段)、４１…通信

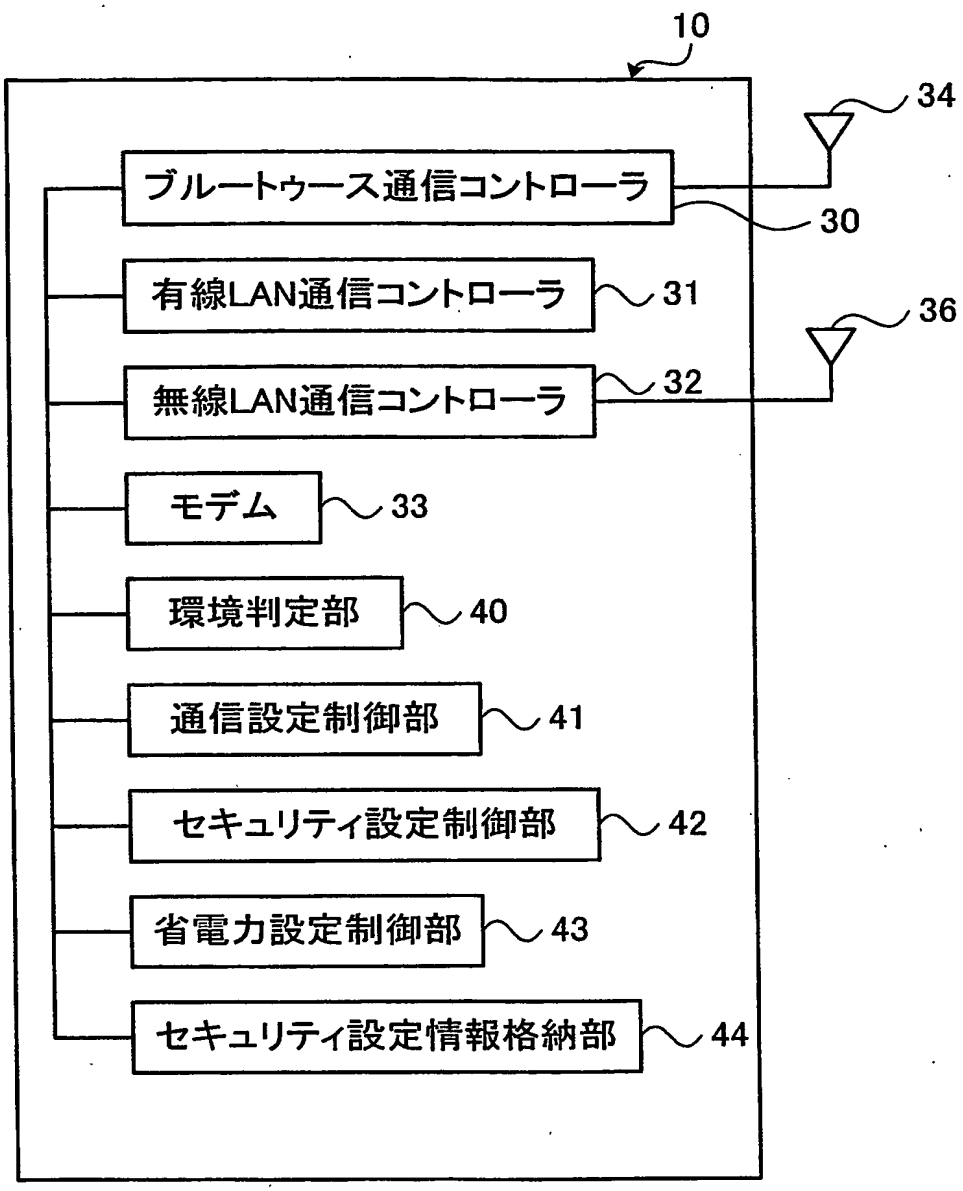
設定制御部、４２…セキュリティ設定制御部(設定変更手段)、４３…省電力設定制御部(設定変更手段)、４４…セキュリティ設定情報格納部

【書類名】　図面

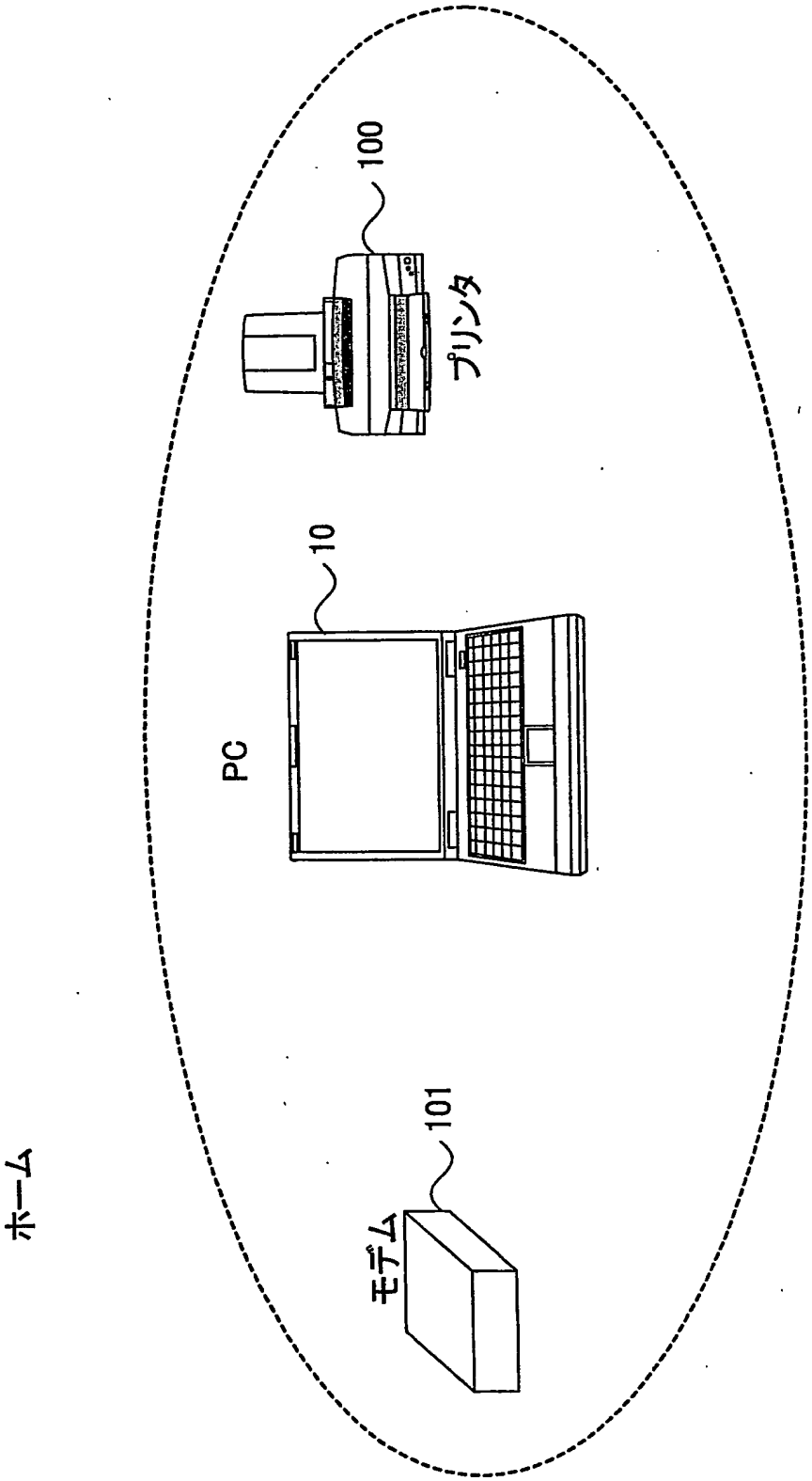
【図１】


10
CPU
11
チップセット
15
メモリ
12
グラフィックチップ
14
LCD
13
PCI BUS
16
ブリッジ回路
22
CMOS
HDD
17
18
EEPROM
21
コントローラ
20
キーボード
19
USB
ブルートゥース通信コントローラ
30
34
25
24
有線LAN通信コントローラ
31
ジャック
35
無線LAN通信コントローラ
32
36
モデム
33
ジャック
37
50

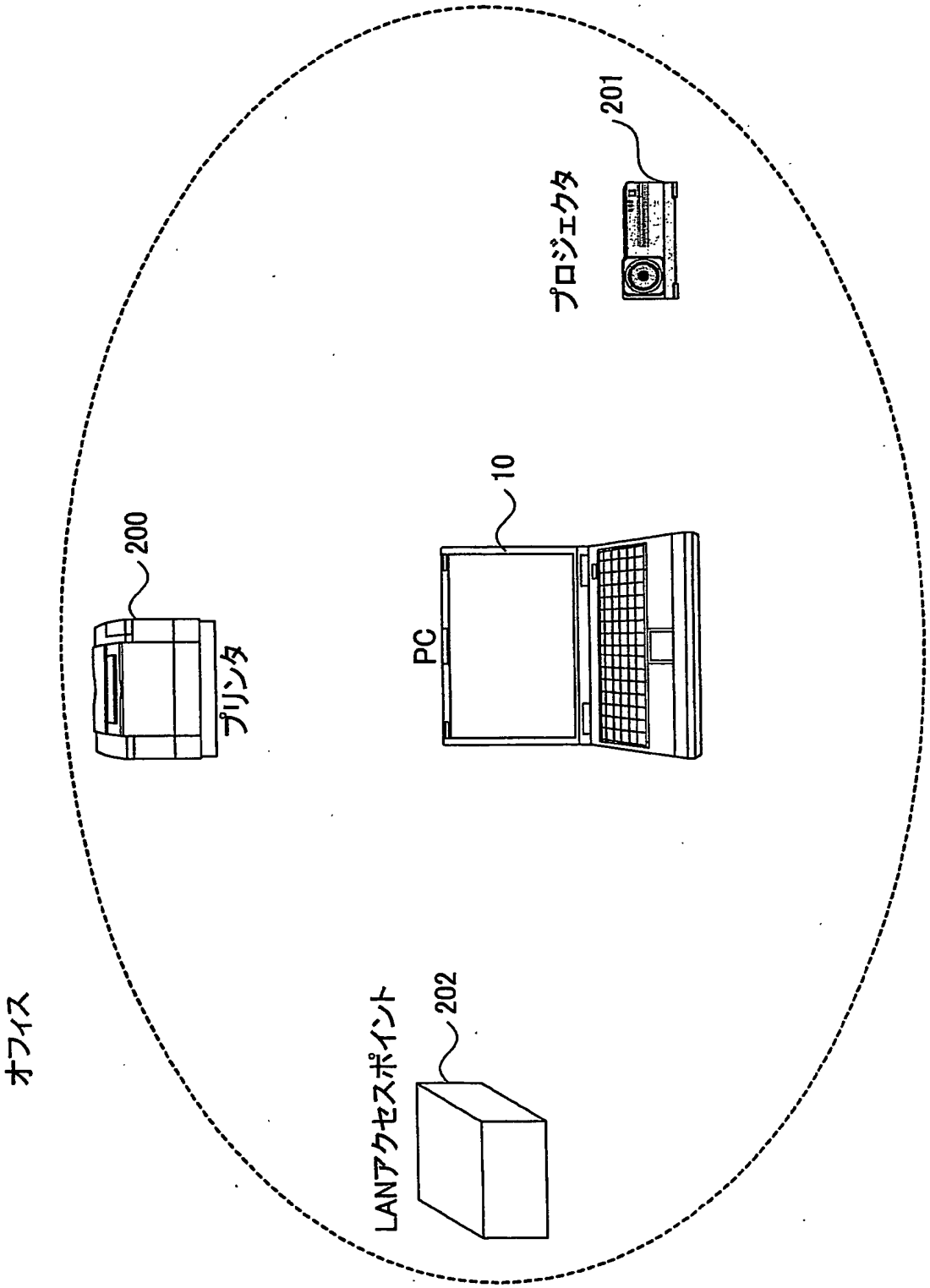
【図２】


10
34
ブルートゥース通信コントローラ
30
有線LAN通信コントローラ
31
36
無線LAN通信コントローラ
32
モデム
33
環境判定部
40
通信設定制御部
41
セキュリティ設定制御部
42
省電力設定制御部
43
セキュリティ設定情報格納部
44

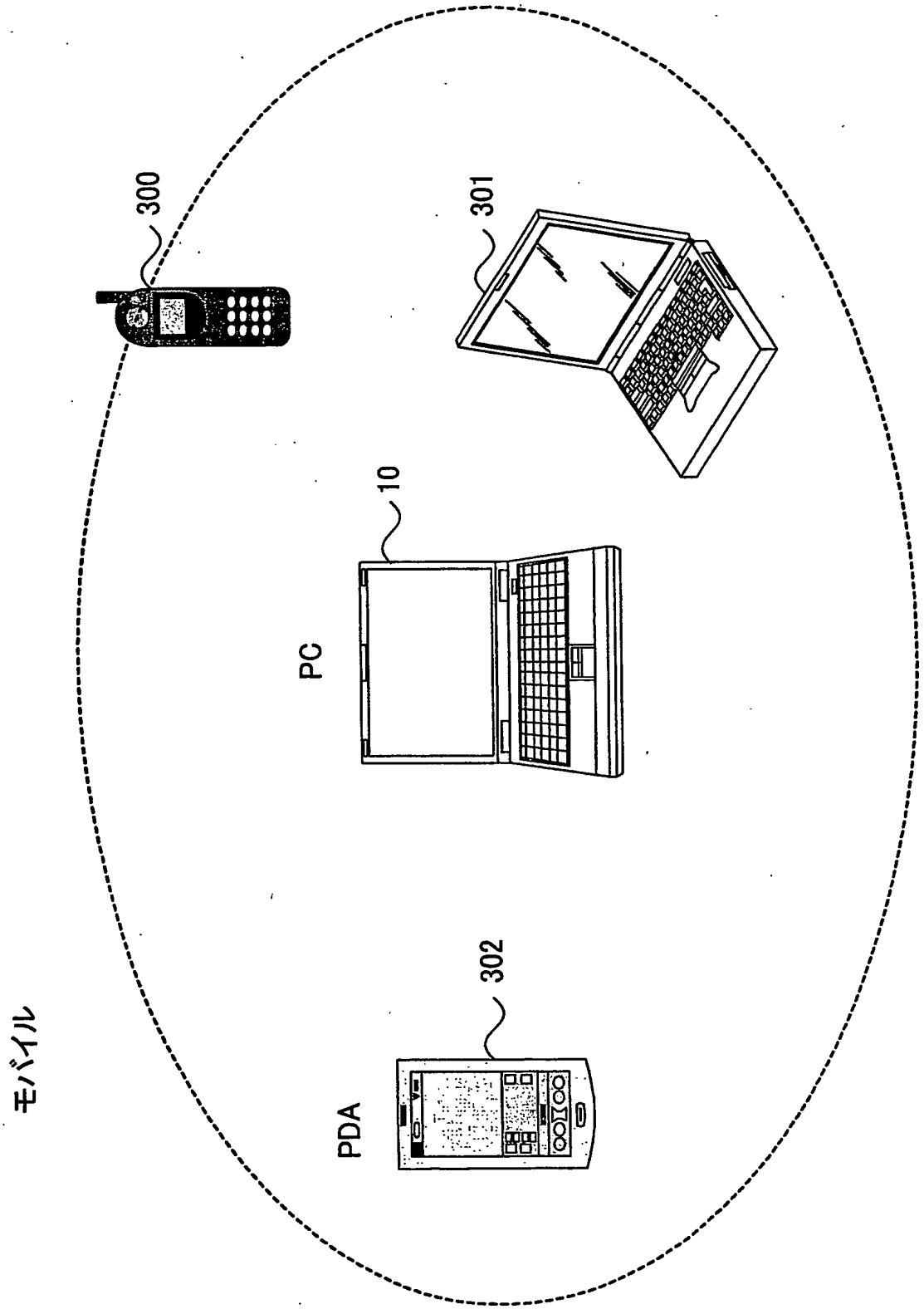
【図３】



【図４】



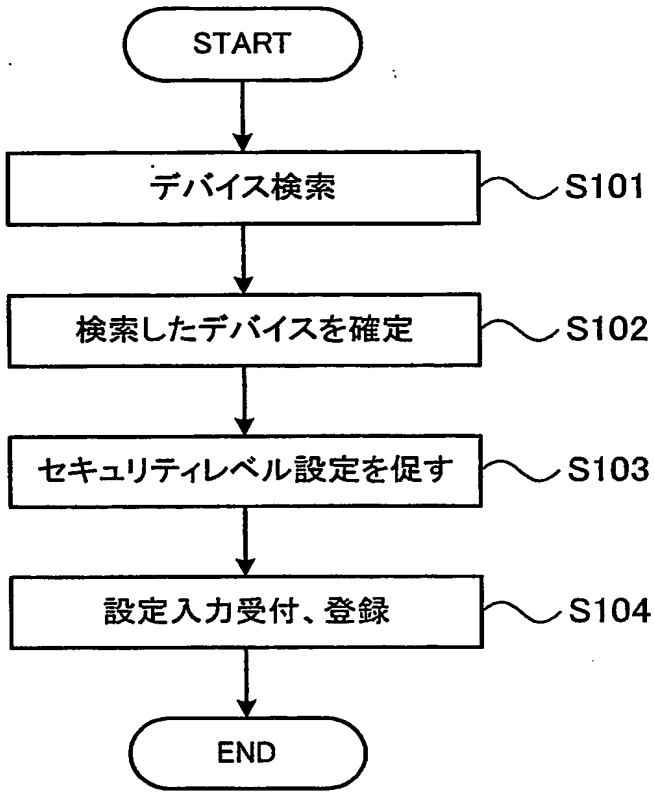
【図５】



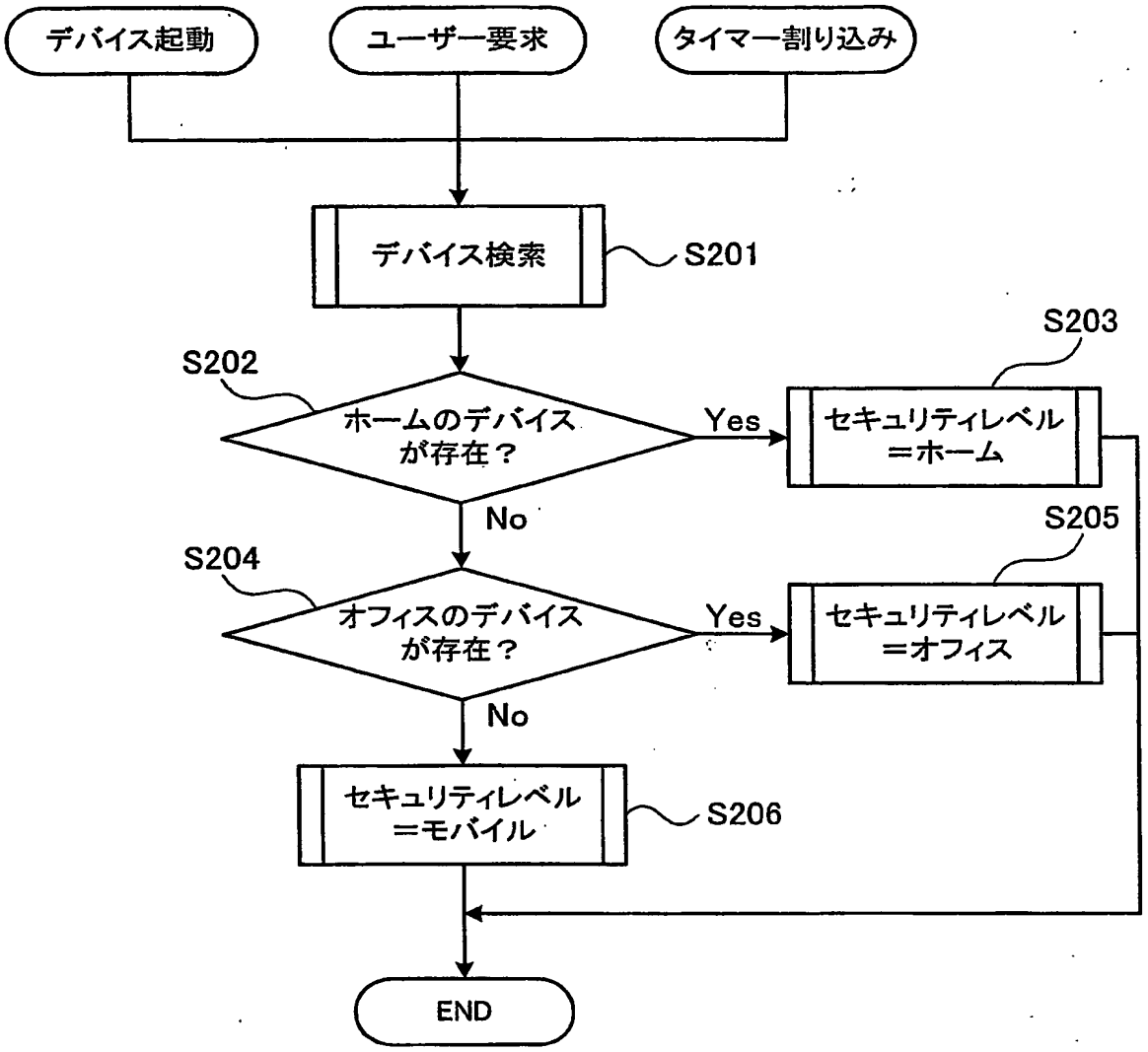
【図６】

セキュリティレベル	他のデバイスからの接続			他のデバイスへの接続		
	認証	許可	暗号化	認証・許可	暗号化
ホーム	必須	——	必須	要求があったとき	要求があったとき
オフィース	必須	必須	必須	要求があったとき	要求があったとき
モバイル	拒否		必須	必須	必須

【図７】


START
デバイス検索
S101
検索したデバイスを確定
S102
セキュリティレベル設定を促す
S103
設定入力受付、登録
S104
END

【図８】


デバイス起動
ユーザー要求
タイマー割り込み
デバイス検索
S201
S202
ホームのデバイス
が存在？
Yes
S203
セキュリティレベル
＝ホーム
No
S204
オフィスのデバイス
が存在？
Yes
S205
セキュリティレベル
＝オフィス
No
セキュリティレベル
＝モバイル
S206
END

【書類名】　　要約書

【要約】

【課題】　使用環境に応じて確実に設定変更を行うことのできる技術を提供し、セキュリティ性の高いネットワーク接続環境を常に確保する。

【解決手段】　ＰＣでは、ブルートゥースを用い、周辺に存在するデバイスのＢＤアドレスを検索することによって、ＰＣの使用環境を判定し、その使用環境に応じてセキュリティレベルの設定を自動的に変更するようにした。さらに、使用環境を判定する処理において、セキュリティレベルを「ホーム」や「オフィス」とすべき使用環境にＰＣがあるときであっても、その使用環境に存在すべきデバイスが検出されないときには、セキュリティ性の高い「モバイル」のセキュリティレベルを設定するようにした。

【選択図】　　図８

認定・付加情報

特許出願の番号	特願２００２－１０９７１４
受付番号	５０２００５３１３００
書類名	特許願
担当官	井筒　セイ子　　１３５４
作成日	平成１４年　６月　４日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【代理人】
- 【識別番号】 100106699
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社大和事業所内
- 【氏名又は名称】 渡部　弘道

【復代理人】 申請人
- 【識別番号】 100104880
- 【住所又は居所】 東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所
- 【氏名又は名称】 古部　次郎

【選任した復代理人】
- 【識別番号】 100100077

次頁有

認定・付加情報（続き）

【住所又は居所】　東京都千代田区岩本町１丁目４番３号　ＫＭビル８階　大場国際特許事務所

【氏名又は名称】　大場　充

次頁無

出証特２００３－３０２５４６４

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション

２．変更年月日　　２００２年　６月　３日
［変更理由］　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション